



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

DICTAMEN N° 11/2004

1. Antecedentes

1.1 Las presentes actuaciones se inician con Nota TI N° 32/2004, de fecha 30 de Septiembre del corriente año, remitida por el Sr. Jefe del Departamento de Informática y Tecnología del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, elevando a ésta el Proyecto de Resolución sobre "Política de uso Aceptable de la Red y de Internet".-

1.2 Dicho Proyecto tiene por objeto reglamentar el uso de los recursos informáticos del Poder Judicial de la Ciudad Autónoma de Buenos Aires.-

1.3 A fs. 2/12 el Señor Jefe de Departamento Informática y Tecnología adjunta el Proyecto de Resolución y su Anexo.-

2. Consideraciones

2.1. En primer lugar, cabe destacar que, de acuerdo a lo expuesto por el Departamento de Informática y Tecnología, este requerimiento se realiza para brindar un mejor servicio, atendiendo las necesidades de los usuarios del Poder Judicial de la Ciudad Autónoma de Buenos Aires, tanto en su rol administrativo, como jurisdiccional.-

2.2 Establece que Internet constituye la herramienta más ventajosa para el acceso y transmisión de información, siendo uno de los medios de mayor alcance que se puede utilizar para difundir información acerca de las actividades y programas que lleva adelante el Poder Judicial de la Ciudad.-

2.3. Es necesario establecer las pautas de uso de los recursos informáticos por parte de los empleados y funcionarios del Poder Judicial de la ciudad, reconociéndolos como individuos responsables.-

3. Conclusiones

3.1. En orden a lo manifestado, esta Comisión estima que habida cuenta la urgencia del requerimiento efectuado, se hace necesario la aprobación de la "Política de Uso Aceptable de los Servicios de la Red y de Internet".-



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

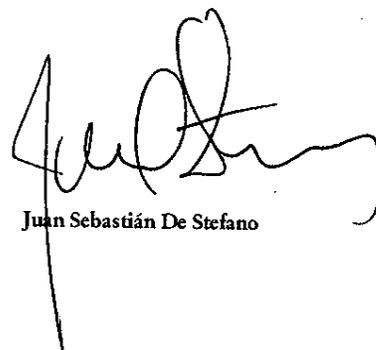
3.2. En consecuencia se elevan las presentes a consideración del Plenario de Consejeros, propiciando el dictado de una resolución en el sentido solicitado, cuyo proyecto se acompaña

Ciudad Autónoma de Buenos Aires, de ~~14 de Mayo~~ de 2004.

DICTAMEN N° 11 /2004 SRⁿ no inespere! Vale -


Carla Cavaliere

Diego May Zubira
Momentaneamente vacante


Juan Sebastián De Stefano



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

Buenos Aires, de Octubre de 2004.-

RES. N° /2004

VISTO:

La Resolución CM N° 459/2000, y

CONSIDERANDO:

Que mediante dicha norma se aprobó, como Anexo I, las “Normas Básicas de Seguridad Informática”, por entender necesaria la preservación del patrimonio del Poder Judicial de la Ciudad Autónoma de Buenos Aires, con excepción del Superior Tribunal de Justicia, en particular de sus bienes informáticos.

Que el Poder Judicial de la Ciudad Autónoma de Buenos Aires, con excepción del Superior Tribunal de Justicia, se encuentra inmerso en un Plan de Sistemas y actualización tecnológica, incorporándose a su ámbito, en los últimos años, herramientas tecnológicas, las cuales han abierto nuevas oportunidades para su empleo en las actividades del personal que los compone, facilitándoles su trabajo al mismo tiempo que permitiendo una mejor prestación de servicios.

Que particularmente Internet constituye la herramienta más ventajosa para el acceso y transmisión de información, siendo uno de los medios de mayor alcance que se puede utilizar para difundir información acerca de las actividades y programas que lleva adelante el Poder Judicial de la Ciudad Autónoma de Buenos Aires, con excepción del Tribunal Superior de Justicia.

Que el área administrativa del Poder Judicial de la Ciudad Autónoma de Buenos Aires promueve el uso de Internet y de su Red Informática Interna para que los empleados y funcionarios realicen trabajos específicos relativos a su función, alentando, tanto



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

a los agentes, funcionarios y magistrados, como al personal contratado a desarrollar habilidades y conocimientos en el uso de dichas herramientas.

Que es necesario establecer las pautas de uso de los recursos informáticos mencionados por parte de los empleados del Poder Judicial de la Ciudad Autónoma de Buenos Aires, con excepción de los que revisten ante el Superior Tribunal de Justicia, reconociéndolos como individuos responsables cuya participación es clave para lograr un accionar acorde con las responsabilidades y acciones asignadas.

Que resulta conveniente delinear una Política de Uso Aceptable por parte de los agentes, funcionarios y magistrados del Poder Judicial de la Ciudad Autónoma de Buenos Aires, cuando utilicen equipamiento, software, nombres de dominio o direcciones de Internet de propiedad del Estado.

Que la Ley Marco N° 25.164 de Regulación de Empleo Público Nacional, establece los derechos y garantías a los trabajadores que integran el servicio civil de la Nación.

Que el artículo 23 del Decreto N° 1421/02, reglamentario de la Ley antes mencionada, determina que entre otras obligaciones, los agentes deberán "...efectuar sus tareas de acuerdo con las modalidades de tiempo, forma y lugar que se deriven de las reglamentaciones pertinentes, ajustando su accionar a las instrucciones que el superior jerárquico emita en el marco de la normativa vigente y las directivas que imparta dentro de su competencia a los efectos de orientar la gestión del área."

Que el Decreto N° 66/99, que aprobó el Convenio Colectivo de Trabajo, el cual establece en su artículo 34, inciso i) entre las prohibiciones que alcanzan a los empleados públicos, la de "hacer uso indebido o con fines particulares del patrimonio estatal". En idéntico sentido se han pronunciado la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, la Ley de Ética en el Ejercicio de la Función Pública N° 25.188 y el Código de Ética de la Función Pública.

Que la Ley 471 de Relaciones Laborales en la Administración Pública de la Ciudad Autónoma de Buenos Aires, en su artículo 10, parte pertinente, prescribe entre las obligaciones de los trabajadores de la Ciudad Autónoma de Buenos Aires las siguientes: "...prestar personal y eficientemente el servicio en las condiciones de tiempo, forma, lugar y



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

modalidad determinados por la autoridad competente, sea en forma individual o integrando los equipos que se constituyan conforme a las necesidades del servicio encuadrando su cumplimiento en principios de eficiencia, eficacia y productividad laboral...”, “... observar en el servicio una conducta correcta, digna y decorosa acorde con su jerarquía y función...”, “...guardar la discreción correspondiente con respecto a todos los hechos e informaciones de los cuales tenga conocimiento durante el ejercicio de sus funciones o con motivo de éste, salvo que aquellos impliquen la comisión de un delito de acción pública...”, “...observar el deber de fidelidad que se derive de la índole de las tareas desarrolladas...”, “...velar por el cuidado y conservación de los bienes de patrimonio de la Ciudad...”.

Que resulta conveniente determinar el ámbito de aplicación de la Política de Uso Aceptable, sugiriendo instruir a funcionarios y magistrados responsables de las distintas áreas y/o dependencias, cuyos subordinados utilizan los recursos informáticos del Poder Judicial de la Ciudad, a fin de dar a conocer, notificar, y exigir su cumplimiento.

Por ello, y en ejercicio de las atribuciones conferidas por el art. 116° de la Constitución de la Ciudad Autónoma de Buenos Aires y La Ley N° 31,

**EL CONSEJO DE LA MAGISTRATURA
DE LA CIUDAD AUTONOMA DE BUENOS AIRES**

RESUELVE:

Art. 1°: Derogar la Resolución CM N° 459/2000 sobre “Normas básicas de seguridad informática”.

Art. 2°: Aprobar la “Política de Uso Aceptable de los Servicios de la Red y de Internet” que como Anexo I forma parte de la presente.

Art. 3°: Instruir a los Magistrados, Funcionarios y responsables de todas las dependencias, cuyos subordinados utilizan los recursos informáticos del Poder Judicial de la Ciudad Autónoma de Buenos Aires, con excepción del Tribunal Superior de Justicia, para acceder a los servicios de la Red y a Internet, para que den a conocer y notifiquen el contenido de la presente Resolución al personal de las respectivas áreas y a exigir su cumplimiento.



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

Art. 4º: Instruir a la Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones y, a través de ella, al Departamento de Tecnología e Informática para que disponga las futuras actualizaciones a la Política mencionada en el artículo 1º, debiendo estar su última versión disponible en la Intranet del Poder Judicial de la Ciudad Autónoma de Buenos Aires.

Art. 5º: La presente medida entrará en vigencia a partir de su publicación.

Art. 6º: Regístrese, publíquese en el Boletín Oficial de la Ciudad de Buenos Aires, en la página de Internet del Poder Judicial de la Ciudad Autónoma de Buenos Aires, notifíquese a los interesados, y oportunamente, archívese.

RESOLUCIÓN Nº /2004

Juan Sebastián De Stefano Diego May Zubiría Bettina Paula Castorino

María Celia Marsili L. Carlos Rosenfeld María Magdalena Iraizóz

Carlos Francisco Balbín Carla Cavaliere Germán C. Garavano



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

ANEXO I

RESOLUCIÓN CM N° /2004

Política de Uso Aceptable de los Servicios de la Red y de Internet

1.- Introducción

El Poder Judicial de la Ciudad Autónoma de Buenos Aires promueve el uso de Internet para que los empleados, funcionario y magistrados realicen trabajos específicos a su función y alienta a todos sus agentes y personal contratado a desarrollar habilidades y conocimiento en su uso.

Este documento establece las normas de conducta razonable que deben observar los agentes y funcionarios del Poder Judicial de la Ciudad Autónoma de Buenos Aires, con excepción del Tribunal Superior de Justicia, cuando utilicen equipamiento, software, direcciones de Internet o nombres de dominio de éstos últimos o cualquier otro recurso informático, teniendo por finalidad la minimización de todos aquellos riesgos que hagan incurrir en responsabilidad a este Consejo.

2.- Objeto

Esta política se aplica a los servicios de la red y de Internet y, más específicamente, al acceso a dicha red y al uso del correo electrónico, cualquiera sea el horario en que se efectúe. No cubre los requerimientos, estándares y procedimientos para el desarrollo e implementación de sitios de información en Internet pertenecientes al Organismo.

3- Sujetos comprendidos

Esta política alcanza a los siguientes usuarios de Internet:

- a) Agentes y funcionarios de planta permanente del Organismo.
- b) Personal contratado que esté autorizado a usar equipos y/o software del Organismo.



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

NOTA: Se encuentra expresamente prohibido el acceso a la red, a Internet o al correo electrónico del Poder Judicial de la Ciudad Autónoma de Buenos Aires a toda otra persona ajena al Organismo, excepto expresa autorización de un funcionario, agente o personal contratado por la institución, en cuyo caso caerá bajo su responsabilidad toda consecuencia legal, de naturaleza administrativa o judicial emanada de dicha autorización.

4.- Reglas generales

Los sistemas de computación del Organismo sólo pueden ser utilizados para propósitos de uso oficial.

Los agentes y funcionarios deberán utilizar Internet para mejorar su conocimiento del trabajo; para acceder a información científica, técnica, o toda otra relativa a temas que tengan relevancia para el Organismo, comunicándose para ello con otras Organizaciones Públicas, Instituciones Académicas y con el Sector Privado en general.

Los usuarios deben tomar conocimiento que las direcciones de correo electrónico, direcciones IP(1) y nombres de dominio y demás recursos perteneciente al Organismo, incluyendo la información almacenada, constituyen bienes intangibles de valor económico de propiedad del mismo, por lo que toda utilización de los mismos será considerada como realizada en su representación, salvo que expresamente se dejare aclarado que dicha utilización y sus consecuencias no constituyen la posición oficial del Organismo. Es indispensable que no se utilice Internet para propósitos que puedan influir negativamente en la imagen del Organismo o de sus autoridades y agentes.

5.- Derechos de los usuarios

Los usuarios podrán realizar las siguientes actividades:

- a) Acceder a información relacionada con su función.
- b) Utilizar el correo electrónico, listas de discusión y otros servicios, siempre que tengan relación directa con la función del agente en el Organismo. Si se expresan opiniones personales, debe aclararse que esa no es la posición oficial del Organismo.



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

6.- Prohibiciones o usos inaceptables

No se permiten los siguientes usos de Internet, utilizando equipamiento del Organismo, en ejercicio o en ocasión de las funciones que se revistan dentro del mismo durante el horario laboral o fuera del mismo:

PROHIBICIONES GENERALES

- a) El acceso no autorizado a sistemas de cómputo o a la red del Organismo o bien transgredir la autorización que como usuario restringido se hubiere otorgado.
- b) La violación de los derechos de privacidad de terceras personas.
- c) La transmisión de amenazas, material obsceno o de hostigamiento.
- d) La transmisión de publicidad no deseada.
- e) La corrupción o destrucción de datos o cualquier acción que pueda impedir el acceso legítimo a los datos, incluyendo la carga de un virus, de gusanos o de cualquier software dañino en cualquier sistema de cómputo conectado a la red.
- f) Cualquier uso condenado por las políticas de uso aceptable de la red conectada.
- g) Cualquier conducta ilegal contraria a la legislación aplicable de cualquier país al que se pueda tener acceso por la red.
- h) Utilización de la red para juegos recreativos.
- i) Distribuir material por Internet que causen daños como la piratería, sabotaje y más específicamente la distribución de software dañino.

PROHIBICIONES PARTICULARES



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

En particular y a los fines relacionados con el cumplimiento de la función desempeñada en el Organismo no se podrá:

- a) Efectuar el downloading (2) de archivos, salvo que esta posibilidad no implique vulnerar o infringir los derechos de terceros titulares de derechos de autor. Entiéndase por “downloading”, el proceso consistente en “bajar” a través de internet u otras redes, archivos de programas, etc. desde una computadora cualquiera a la propia
- b) Realizar cualquier actividad contraria a los intereses del Organismo, tal como publicar información reservada, acceder sin autorización a recursos o archivos o impedir el acceso a otros usuarios mediante el mal uso deliberado de recursos comunes.
- c) Utilizar la red para propósitos no relacionados con las actividades del Organismo, prohibiéndose su utilización para el desarrollo de cualquier actividad comercial personal en Internet, ya sea la compra, venta u oferta de bienes o servicios o bien utilizar la red para la transmisión de publicidad comercial relacionada con dicha actividad.
- d) Utilizar la red para conducir al personal a la realización de actividades lucrativas.
- e) Iniciar cualquier actividad que pueda comprometer la seguridad de los servidores del Organismo.
- f) Dar autorización o permiso a una persona no conectada a la red del Organismo para que la utilice ilegalmente.
- g) Revelar a terceros contraseñas de acceso(3) o compartirlas con otros usuarios.
- h) Realizar cualquier actividad de recaudación de fondos.
- i) Realizar cualquier actividad de recreación personal o de promoción de intereses personales (tales como creencias religiosas, hobbies, etc.).
- j) Iniciar sesiones de Internet(4) usando recursos del Organismo desde ubicaciones remotas, salvo que estén especialmente autorizados para ello.



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

7.- Responsabilidades de los Superiores

Los superiores de los agentes y del personal contratado tendrán las siguientes responsabilidades:

- a) Evaluar la necesidad de los agentes de acceder a Internet para cumplir con sus funciones, contemplando aquellas situaciones donde el requerimiento se encontrare dirigido a obtener información técnica sobre determinado producto o bien a obtener ayuda en línea.
- b) Obtener acceso a Internet para los agentes que lo necesiten en razón de sus funciones debiendo cumplirse en cuyo caso con las normas de procedimiento que habilitan el acceso a Internet publicadas por la Oficina Nacional de Tecnologías de Información.
- c) Autorizar excepcionalmente el acceso a Internet en días no laborables para propósitos relacionados con la función que el agente cumple dentro del Organismo, estableciéndose como regla general la imposibilidad de acceso en las referidas circunstancias.
- d) Difundir entre el personal las restricciones en el uso personal de los recursos con los que cuenta el Organismo para acceder a los servicios de Internet, guardando copia de las respectivas notificaciones.
- e) Asegurar que el personal conozca esta Política de Uso Aceptable y llamar su atención cuando tome conocimiento de su falta de cumplimiento.
- f) Poner en conocimiento del personal las sanciones que les podrían corresponder, -(desde llamado de atención, prohibición de acceso a Internet hasta el inicio de las correspondientes acciones administrativas y/o judiciales)-, como consecuencia de su incumplimiento.
- g) Notificar al administrador de la red cuando un agente deja de prestar servicio en el Organismo para que sus cuentas sean deshabilitadas.

8.- Responsabilidades de los Usuarios

Para evitar problemas de falta de recursos y garantizar la seguridad física y lógica de los mismos, los usuarios de la red y de Internet tendrán las siguientes responsabilidades:



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

- a) Conocer y aplicar lo establecido en la Política de Uso Aceptable.
- b) Seguir las políticas y procedimientos de seguridad existentes para el uso de los servicios de la red y de Internet (5) y evitar toda práctica que pueda dañar los sistemas de computación y archivos de datos del Organismo, como por ejemplo, aquellos que puedan dar lugar a ataques de virus cuando se recuperen archivos de Internet.
- c) Limitar sus comunicaciones con terceros a los temas respecto de los cuales tienen conocimiento y responsabilidad profesional.
- d) Identificarse adecuadamente en toda comunicación con terceros, indicando su nombre, dirección electrónica y Organismo al que pertenecen.
- e) Conducirse de forma que refleje positivamente la imagen del Organismo, ya que se encuentran identificados como empleados del mismo.
- f) Cumplir las indicaciones y pautas establecidas por el Organismo para reducir los problemas de seguridad así como el impacto de virus en la red.

9.- Correo electrónico

La utilización del correo electrónico como medio de transmisión de información por parte de los agentes y funcionarios del Poder Judicial de la Ciudad Autónoma de Buenos Aires debe favorecerse, teniendo en cuenta sus notorias ventajas sobre los medios tradicionales (economía, rapidez, eficiencia y confiabilidad).

El uso del correo electrónico resulta el más apropiado cuando el usuario:

- a) No tiene urgencias en recibir una respuesta y/o en ubicar al receptor.
- b) Desea enviar el mensaje a más de un receptor.
- c) Necesita información específica sobre determinados temas.



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

d) Necesita dejar evidencia escrita respecto de los mensajes transmitidos.

Sin embargo, sus características también exigen un comportamiento responsable por parte de los usuarios, con el fin de convertirlo en un sistema ágil y seguro.

Es responsabilidad de los superiores notificar al administrador de la red cuando un agente deja de prestar servicio en el Organismo para que su cuenta de correo sea deshabilitada.

En general, los usuarios del sistema de correo electrónico deben:

a) Tomar conciencia que el correo electrónico y la cuenta de e-mail que se les hubieren proporcionado por el Organismo para el cumplimiento de sus tareas son de titularidad del mismo independientemente del nombre y clave de acceso que fueren necesarias para su utilización.

b) Asumir una absoluta responsabilidad respecto al contenido de todo mensaje que envíen utilizando los recursos o medios proporcionados por el Organismo. Estos deben ser explícitos y concisos, escritos en un tono amable y utilizando un lenguaje adecuado, que no exceda los límites del buen gusto, la moral y las buenas costumbres.

c) Transmitir y almacenar información considerada confidencial solo en caso de encontrarse debidamente autorizados.

d) Evitar en todos los casos la divulgación de sus claves o contraseñas de acceso personales.

e) Verificar diariamente sus casillas electrónicas, evitando la acumulación de mensajes en ellas. En este sentido se advierte que debido a políticas internas relativas a la administración de los recursos informáticos, al exceder determinado volumen dichos mensajes serán eliminados automáticamente.

f) Tener en cuenta que al utilizar las direcciones de correo electrónico del Organismo están actuando en su representación. Si las opiniones que expresan son a título personal, deben aclarar que esa no es la posición oficial del Organismo. A tal fin deberá incluirse al pie de los mensajes de correo electrónico la siguiente leyenda: "El mensaje precedente es privado y en consecuencia confidencial y solamente para la dirección electrónica y persona a la que está



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

dirigido. Si ha recibido este mensaje por error, no debe revelar, copiar, distribuir o usar su contenido. La transmisión errónea del mensaje no implica la renuncia a la confidencialidad ni a ningún otro derecho. Asimismo, esta Oficina no se hace responsable por los cambios, omisiones, alteraciones y/o errores que pudiera sufrir el mensaje luego de ser enviado. Se deja constancia que el contenido de este mensaje no necesariamente expresa la opinión de la Oficina Nacional de Tecnologías Informáticas."

Se deja constancia que respecto al correo electrónico rige la misma política de monitoreo establecida para Internet y la red en el punto 8 dejándose asimismo constancia que de ninguna manera se procederá a la comprobación o interceptación de los contenidos de los e-mails de los agentes sino existen razones de amenaza para el funcionamiento y/o seguridad del Organismo al cual representan o bien razones de orden judicial.

10.- Uso de Claves de Acceso

Las Claves de Acceso constituyen un elemento fundamental de la seguridad. Son la primera protección de las cuentas de usuario. Una Clave de Acceso inapropiada puede comprometer a toda la red institucional del Poder Judicial de la Ciudad. Por lo tanto, todos los usuarios de los sistemas de este Organismo (incluyendo a terceros con acceso a estos sistemas) son responsables de adoptar las medidas que aseguran un correcto empleo de sus Claves de Acceso.

Procedimientos

- Todas las Claves de Acceso a nivel de sistema (por ejemplo: root, Administradores NT /W2003 y cualquier otra forma de administración) deben ser cambiadas periódicamente.
- Todas las Claves de Acceso de los sistemas en producción deben ser administradas en forma global.
- Todas las Claves de Acceso a nivel de usuarios (por ejemplo: Correo electrónico, acceso a la red o a los puestos de trabajo) deben ser cambiadas como mínimo cada seis meses. El intervalo recomendado es cada cuatro meses.
- Las Claves de Acceso no deben ser transmitidas vía correo electrónico u otras formas de comunicación electrónica.



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

- Todas las Claves de Acceso tanto a nivel de usuario como de sistema deben conformarse según las instrucciones que se destacan a continuación.

Para la construcción de Claves de Acceso se debe utilizar Claves de Acceso apropiadas (fuertes) para toda identificación que sea permanente y para toda cuenta de usuario asignada por el Organismo.

Una Clave de Acceso débil o inapropiada se caracteriza por:

- Contener menos de ocho caracteres.
- Puede ser encontrada en un Diccionario.
- Es un nombre propio, por ejemplo:
 - Nombres de familiares, mascotas, amigos, compañeros de trabajo, personajes públicos y otros de este tipo.
 - Términos y nombres de computadoras, sitios, empresas, sistemas y/o equipamiento,
 - Fechas de cumpleaños y cualquier otra información personal, tales como direcciones y números telefónicos.
 - Combinaciones con letras repetidas o secuenciales del tipo aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Todas las anteriores escritas en orden inverso.
 - Todas las anteriores precedidas o seguidas por un número (por ejemplo, secret1, 1secret).

Las Claves de Acceso apropiadas (fuertes) se caracterizan por:

- Contienen caracteres en Mayúsculas y Minúsculas (i.e.: a-z, A-Z)
- Contienen dígitos y signos de puntuación además de letras (i.e.: , 0-9, !@#\$%^&*()_+|~=\`{}[]:;'\<>?,./)
- Tienen un mínimo de ocho caracteres.
- No son palabras que pertenecen a ningún idioma o dialecto.
- No están basadas en información personal.
- Las Claves de Acceso nunca deben ser escritas o almacenadas en línea. Trate de crear Claves de acceso que sean fáciles de recordar. Una manera es usar cierta frase conocida como referencia, por ejemplo la frase “Yo te saludo mañana” puede generar la clave YtSalu2mña.



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

Protección de Claves de Acceso.

- No utilice la misma clave empleada en el ámbito del Organismo en otros ambientes. Si necesita utilizar mas de una clave en el CMCABA trate de que sean diferentes.
- Jamás revele su clave vía telefónica a nadie.
- Jamás revele su clave en un mensaje de correo.
- No le proporcione su clave a sus superiores.
- No hable sobre sus claves con otros.
- No revele su clave en cuestionarios o formularios de ningún tipo.
- No comparte su clave con familiares.
- No revele su clave a sus compañeros de trabajo al irse de vacaciones.
- Si alguien le pide su clave refiera a la estos procedimientos.
- No comparta con nadie su clave de acceso, incluyendo a personal administrativo, asistentes o secretarias. Todas las claves deben ser tratadas como información sensitiva y secreta del Organismo.

Tenga siempre presente la siguiente lista de sugerencias:

No utilice las facilidades de “Recuerde la Clave” encontradas en ciertas aplicaciones.

Nuevamente repetimos que las claves no deben ser escritas ni guardadas en ninguna computadora o medio magnético sin antes ser encriptadas.

En forma aleatoria este Organismo puede analizar la factibilidad de “romper” (buscar hasta encontrar) su clave. Si esto ocurre Usted será notificado y deberá proceder al cambio de la misma en forma inmediata.

Estándares para el Desarrollo de Aplicaciones

Los desarrolladores de aplicaciones deben asegurar que las aplicaciones desarrolladas / implementadas contemplen los criterios de seguridad siguientes:

- La autenticación debe ser realizada a nivel de usuarios y no grupos.
- Las Claves de Acceso no deben ser almacenadas sin previa encriptación.



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

- Deben permitir el uso de roles que eviten recurrir al uso de la clave de un usuario en particular para completar tareas rutinarias.
- Deberán soportar autenticación vía TACACS+ , RADIUS y/o X.509 con LDAP , siempre que sea posible.

Uso de Claves de Acceso y Frases para acceso remoto de usuarios

El acceso a la red del Organismo vía remota deberá ser controlado sea mediante claves válidas para un único uso o utilizando sistemas de Claves Públicas provisto de frases claves fuertes.

Frases Claves

Las Frases Claves son generalmente utilizadas en los procesos de autenticación de claves pública / privada. Un sistema de claves pública / privada define una relación matemática entre la clave pública (conocida) y la privada (conocida solo por el usuario). Las Frases Claves se utilizan para acceder a la clave privada.

Las Frases Claves no son lo mismo que las Claves de Acceso. La Frase Clave es una versión más larga que una clave común y por lo tanto más segura. La Frase Clave esta compuesta por múltiples palabras.

Todas las reglas enumeradas para la evaluación y construcción de Claves de Acceso son válidas a la hora de definir Frases Claves.

11.-Responsabilidad del Administrador de correo electrónico

El Administrador de correo electrónico del Organismo no podrá, bajo ninguna circunstancia, retener, desviar, divulgar o alterar mensajes que no estén dirigidos específicamente a su dirección.

Deberá proveer los medios para que sea devuelto a su emisor todo mensaje recibido que no pueda ser transferido a su destinatario (por ejemplo, un mensaje con dirección errónea).



Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires
Comisión Auxiliar de Incorporación de Tecnologías de la Información y las Comunicaciones

Además, deberá arbitrar medidas para borrar el cuerpo principal de todo mensaje fallido (es decir, que no pueda ser entregado, cualquiera sea la causa) para luego devolverlo al emisor.

12.- Breve glosario de términos

(1) Direcciones IP: Número que identifica un host (máquina) unívocamente en una red, representado usualmente por cuatro números entre 0 y 255 separados por puntos.

(2) Downloading: Es el proceso para "bajar" (traer) a través de Internet u otras redes, archivos de programas, etc. desde una computadora cualquiera a la propia.

(3) Contraseñas de acceso: Sucesión de letras y números que permiten a un usuario acceder a un servicio de la red.

(4) Sesiones de Internet: Conexiones a Internet realizados por los usuarios

(5) Servicios de Internet: Facilidad que presta el organismo para que los usuarios puedan consultar páginas por Internet, acceder al Correo Electrónico, etc.

Organismo: entiéndase Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.